UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/527,368	01/04/2006	Pasi Ahonen	P17580US1	5719

27045 7590 12/30/2008

ERICSSON INC.
6300 LEGACY DRIVE
M/S EVR 1-C-11
PLANO, TX 75024

EXAMINER	
SU, SARAH	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
12/30/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/527,368	**Applicant(s)** AHONEN ET AL.
	Examiner Sarah Su	**Art Unit** 2431

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 October 2008*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-13 and 15-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-13 and 15-25* is/are rejected.

7)☒ Claim(s) *4,11 and 13* is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *17 October 2008* is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

FINAL ACTION

1. Amendment A, received on 17 October 2008, has been entered into record. In this amendment, claims 1-13 and 15-25 have been amended.

2. Claims 1-13 and 15-25 are presented for examination.

Response to Arguments

3. Regarding the objections to the specification, the applicant has submitted amendments to the specification, and the examiner hereby withdraws the objections.

4. Regarding the objections to the drawings, the applicant has submitted replacement sheets on 17 October 2008, and the examiner hereby withdraws the objections.

5. Applicant's arguments with respect to the rejection of claims 1-13 and 15-25 have been considered but are moot in view of the new ground(s) of rejection.

Drawings

6. The drawings were received on 17 October 2008. These drawings are acceptable.

Claim Objections

7. Claims 4, 11, and 13 are objected to because of the following informalities:

a. In claim 4, line 9: “the source IPv6 address” lacks antecedent basis;

b. In claim 11, lines 8-9: “a certificate” is unclear if it relates to “a certificate” (claim 7, line 5);

c. In claim 13, line 18: “the source IP address” lacks antecedent basis.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1, 3-4, 13, and 16-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nikander (GB 2367986 A) in view of Fox et al. (US Patent 5,790,677 and Fox hereinafter).

As to claims 1 and 13, Nikander discloses a method for IP network authorization using a coded interface identifier, the method having:

> **at the group controller, verifying that the public key received from each candidate member wishing to participate is owned by the candidate member and that the public key is associated with the respective candidate member’s IPv6 address by inspecting an interfaceID part of the IPv6 address** (page 8, lines 21-29)**.**

Nikander does not disclose:

a candidate member receiving an invitation from a group controller to join the multicast;

the candidate member sending a registration message to the group controller, the registration message including the candidate member's originating IPv6 address, a copy of the candidate member's public key from the candidate member's public-private key pair and a digital signature using the candidate member's private key from the candidate member's public-private key pair;

using the digital signature, further verifying that the candidate member owns the public-private key pair to which the public key belongs and that the candidate terminal owns the source IP address.

Nonetheless, these features are well known in the art and would have been an obvious modification of the teachings disclosed by Nikander, as evidenced by Fox.

Fox discloses a system and method for secure electronic commerce transactions, the system and method having:

a candidate member receiving an invitation (i.e. application) **from a group controller to join the multicast** (col. 8, lines 36-39);

the candidate member sending a registration message to the group controller, the registration message including the candidate member's originating IPv6 address (i.e. location)**, a copy of the candidate member's public key from the candidate member's public-private key pair and a**

digital signature using the candidate member's private key from the candidate member's public-private key pair (col. 8, lines 33-35, 39-42);

using the digital signature, further verifying that the candidate member owns the public-private key pair to which the public key belongs and that the candidate terminal owns the source IP address (col. 9, lines 32-43)**.**

Given the teaching of Fox, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Nikander with the teachings of Fox by using an IP address, public key and digital signature for registration. Fox recites motivation by disclosing that safeguards to protect the interests of trading partners and minimize the risk of participants include authenticity, integrity, privacy, and security, which can be accomplished by ensuring that partners are authentic and instruments have integrity (col. 1, lines 30-35). It is obvious that the teachings of Fox would have improved the teachings of Nikander by using an IP address, public key and signature to verify a candidate in order to prove the authenticity of a participant and integrity of the system.

10. Claims 2, 5-6, 15, and 18-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nikander in view of Fox as applied to claims 1, 13 and 17 above, and further in view of Caronni et al. (US Patent 6,049,878 and Caronni hereinafter).

As to claims 2 and 15, Nikander in view of Fox does not disclose:

wherein said key revocation based scheme is a Logical Key Hierarchy based scheme.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Nikander in view of Fox, as evidenced by Caronni.

Caronni discloses a system and method for efficient, secure multicasting with global knowledge, the system and method having:

wherein said key revocation based scheme is a Logical Key Hierarchy based scheme (i.e. binary tree) (col. 6, lines 27-31)**.**

Given the teaching of Caronni, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Nikander in view of Fox with the teachings of Caronni by using a Logical Key Hierarchy based scheme. Caronni recites motivation by disclosing that using a secure distribution tree can allow scalability (col. 3, lines 12-20). It is obvious that the teachings of Caronni would have improved the teachings of Nikander in view of Fox by using a tree distribution scheme in order to allow for scalability in the system.

As to claims 5 and 18, Nikander in view of Fox does not disclose:

wherein, after the group controller has received the public key from a given candidate member and has verified that the public key is associated with the IPv6 address of the sender, the group controller sends a unique Key Encryption Key to the member, encrypted with that member's public

key, and the group controller also sends a Traffic Encryption Key and a LKH key set to the member, encrypted with the Key Encryption Key.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Nikander in view of Fox, as evidenced by Caronni.

Caronni discloses:

> **wherein, after the group controller has received the public key from a given candidate member and has verified that the public key is associated with the IP address of the sender, the group controller sends a unique Key Encryption Key to the member, encrypted with that member's public key, and the group controller also sends a Traffic Encryption Key and a LKH key set to the member, encrypted with the Key Encryption Key** (col. 6, lines 27-37)**.**

Given the teaching of Caronni, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Nikander in view of Fox with the teachings of Caronni by using multiple keys for encryption. Caronni recites motivation by disclosing that using multiple keys allows for the forming of groups by sharing the KEK with particular participants (col. 8, lines 61-63) while the TEK is shared among all participants (col. 6, lines 16-17). It is obvious that the teachings of Caronni would have improved the teachings of Nikander in view of Fox by using multiple keys for encryption in order to allow the forming of groups within the multicast.

As to claims 6 and 19, Nikander in view of Fox does not disclose:

a one-way multicast where a single node multicasts a stream of data to several other nodes;

a group multicast where group members multicast data to all other members of the group; or

a tele-conference or a videoconference or a multimedia conference.

Nonetheless, these features are well known in the art and would have been an obvious modification of the teachings disclosed by Nikander in view of Fox, as evidenced by Caronni.

Caronni discloses:

a one-way multicast where a single node multicasts a stream of data to several other nodes;

a group multicast where group members multicast data to all other members of the group; or

a tele-conference or a videoconference or a multimedia conference (col. 3, lines 34-43).

Given the teaching of Caronni, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Nikander in view of Fox with the teachings of Caronni by using a one-way multicast, a group multicast or a teleconference. Caronni recites motivation by disclosing that multicasting is an effective platform for building group-oriented services (col. 1, lines 34-36). It is obvious that the teachings of Caronni would have improved the teachings of Nikander in view of Fox by allowing for a one-way multicast, a group multicast, or a teleconference in order to create a platform for effective group-oriented services where participants can communicate with other participants.

11. Claims 7-9, 20-22 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wesley et al. (US Patent 6,275,859 B1 and Wesley hereinafter) in view of Caronni and Fruehauf et al. (US Patent 7,149,308 B1 and Fruehauf hereinafter). As to claims 7 and 20, Wesley discloses a system and method for tree-based reliable multicasting, the system and method having:

> **delivering a certificate to the user, the certificate verifying that a public private key pair identified in the certificate can be validly used by the user to access said secure multicast/broadcast, wherein the certificate further includes a digital signature generated by applying an algorithm and the user's private key to the contents of the certificate** (col. 2, lines 13-14; col. 4, lines 15-22)**;**
>
> **subsequently verifying at a control node that the certificate is owned by the user using a proof-of-possession procedure that is based on the private key** (col. 3, lines 6-9; col. 4, lines 19-22)**.**

Wesley does not disclose:

> **distributing security keys to users using a key revocation based mechanism;**

assuming that verification is obtained, using said public key to send a Key Encryption Key to the user.

Nonetheless, these features are well known in the art and would have been an obvious modification of the teachings disclosed by Wesley, as evidenced by Caronni.

Caronni discloses:

assuming that verification is obtained, using said public key to send a Key Encryption Key to the user (col. 6, lines 27-31)**.**

Given the teaching of Caronni, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Wesley with the teachings of Caronni by sending a Key Encryption Key to a user. Please refer to the motivation recited above in respect to claims 5 and 18 as to why it is obvious to apply the teachings of Caronni to the teachings of Wesley.

Wesley in view of Caronni does not disclose:

distributing security keys to users using a key revocation based mechanism.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Wesley in view of Caronni, as evidenced by Fruehauf.

Fruehauf discloses a system and method for cryptographic communications using keys for conditional access, the system and method having:

distributing security keys to users using a key revocation based mechanism (col. 1, lines 64-67)**.**

Given the teaching of Fruehauf, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Wesley in view of Caronni with the teachings of Fruehauf by using a key revocation mechanism. Fruehauf recites motivation by disclosing that conditional access of a user can be revoked by removal of availability of the needed combination of values to that user (col. 3, lines 54-56). It is obvious that the teachings of Fruehauf would have improved the teachings of Wesley in view of Caronni by providing for key revocation in order to control conditional access to a user.

As to claims 8 and 21, Wesley does not disclose:

wherein said key revocation based scheme is a Logical Key Hierarchy based scheme.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Wesley, as evidenced by Caronni, combined with Fruehauf.

Caronni discloses:

wherein said key revocation based scheme is a Logical Key Hierarchy based scheme (i.e. binary tree) (col. 6, lines 27-31)**.**

Given the teaching of Caronni, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Wesley with the teachings of Caronni by using a Logical Key Hierarchy based scheme. Please refer to the motivation recited above in respect to claims 2 and 15 as to why it is obvious to apply the teachings of Caronni to the teachings of Wesley.

As to claims 9 and 22, Wesley discloses:

> **wherein said step of verifying at a control node that the certificate is owned by the user, is carried out after the control node receives a request from the user to join said secure multicast or broadcast** (col. 4, lines 3-6)**.**

As to claim 25, Wesley discloses:

> **wherein an Authentication and Key Agreement (AKA) procedure is used to authorize the user** (col. 2, lines 5-13). The examiner asserts that using a symmetric key authentication on a security protocol would have been functionally equivalent to using an Authentication and Key Agreement procedure. Thus, it would have been obvious to modify the teachings of Wesley with an Authentication and Key Agreement procedure in order to obtain the claimed invention.

12. Claims 10 and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wesley in view of Caronni and Fruehauf as applied to claims 7 and 20 above, and further in view of Nikander.

As to claims 10 and 23, Wesley in view of Caronni and Fruehauf does not disclose:

> **wherein said proof-of-possession procedure involves the control node sending a random number to the user in plain text, and the user sending a response to the control node containing a signature generated by applying the private key to the random number, wherein the control node is in possession of the user's certificate and can check whether or not the message is correctly signed with the user's private key.**

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Wesley in view of Caronni and Fruehauf, as evidenced by Nikander.

Nikander discloses:

> **wherein said proof-of-possession procedure involves the control node sending a random number to the user in plain text** (page 8, lines 5-6, 10)**, and the user sending a response to the control node containing a signature generated by applying the private key to the random number** (page 8, lines 16-18)**, wherein the control node is in possession of the user's certificate and can check whether or not the message is correctly signed with the user's private key** (page 9, lines 3-8).

Given the teaching of Nikander, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Wesley in view of Caronni and Fruehauf with the teachings of Nikander by using a random number and signature to verify if a message is correctly signed. Caronni recites motivation by disclosing that existing multicasting techniques must be supplemented by tools for protecting (i.e. encrypting and authenticating) traffic, controlling participation, and restricting access from unauthorized users (col. 1, lines 37-40). It is obvious that the teachings of Wesley in view of Caronni and Fruehauf would have benefited from the teachings of Nikander by using a random number and signature to verify a message in order to provide protection and security in a multicasting system.

13. Claims 11-12 and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wesley in view of Caronni and Fruehauf as applied to claims 7 and 20 above, and further in view of Chow et al. (US 2003/0053434 A1 and Chow hereinafter).

As to claims 11 and 24, Wesley, combined with Caronni and Fruehauf, discloses:

> **following authorization by the home network, generating a certificate relating to said service and generating the public-private key pair, either at the user equipment or within one of the networks, and signing the certificate** (col. 4, lines 15-22)**;**
>
> **sending the certificate to the user** (col. 4, lines 19-22)**.**

Wesley in view of Caronni and Fruehauf does not disclose:

> **the visited network, in which the user is roaming, contacting the user's home network, upon receipt of an initial registration request from said user, to authorize the user.**

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Wesley in view of Caronni and Fruehauf, as evidenced by Chow.

Chow discloses a system and method for delivering wireless LAN mobile radio service, the system and method having:

> **the visited network, in which the user is roaming, contacting the user's home network, upon receipt of an initial registration request from said user, to authorize the user** (0060, lines 5-14).

Given the teaching of Chow, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Wesley in view of Caronni and Fruehauf with the teachings of Chow by contacting the home network of a roaming user for authorization. Chow recites motivation by disclosing that allowing registration when a subscriber is roaming allows service to be rendered to all subscribers/members/communicators anytime, anywhere and with any device (0060, lines 1-5). It is obvious that the teachings of Chow would have improved the teachings of Wesley in view of Caronni and Fruehauf by authorizing a roaming user in order to ensure that service can be provided to all users without dependence on location or device.

As to claim 12, Wesley, combined with Caronni, Fruehauf and Chow, discloses:

> **wherein an Authentication and Key Agreement (AKA) procedure is used to authorise the user** (col. 2, lines 5-13). The examiner asserts that using a symmetric key authentication on a security protocol would have been functionally equivalent to using an Authentication and Key Agreement procedure. Thus, it would have been obvious to modify the teachings of Wesley with an

Authentication and Key Agreement procedure in order to obtain the claimed invention.

Conclusion

14. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sarah Su whose telephone number is (571) 270-3835. The examiner can normally be reached on Monday through Friday 7:30AM-5:00PM EST..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Sarah Su/
Examiner, Art Unit 2431

/Christopher A. Revak/
Primary Examiner, Art Unit 2431